US-PAT-NO: 6567794
DOCUMENT-IDENTIFIER: US 6567794 B1 **See image for Certificate of Correction**

TITLE: Method for access control in a virtual postage metering system
DATE-ISSUED: May 20, 2003
INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Cordery; Robert A.	Danbury	CT	N/A	N/A
D'Ippolito; Frank M.	Arlington	MA	N/A	N/A

US-CL-CURRENT: 705/60, 705/401 , 705/75

ABSTRACT: A method of remotely accessing a postage security account at a data center from a remote user device begins with a remote user assigning a password to the user's postage security account at a data center. A cryptographic key corresponding to the user's postage security account is provided to the remote user device and is stored at the data center. The password and the cryptographic key are combined at the remote user device and the data center respectively to obtain a user authentication key. An authentication algorithm is performed using the user authentication key to obtain a remote access message. The remote access message is sent to the data center to initiate request for access to the postage security account by the remote user device. The remote user device is authenticated for accessing the postage security account when the data center verifies the remote access message.

13 Claims,   6 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 6

---------- KWIC ----------

Abstract Text - ABTX (1): A method of remotely accessing a postage security account at a data center from a remote user device begins with a remote user assigning a password to the user's postage security account at a data center. A cryptographic key corresponding to the user's postage security account is provided to the remote user device and is stored at the data center. The password and the cryptographic key are combined at the remote user device and the data center respectively to obtain a user authentication key. An authentication algorithm is performed using the user authentication key to obtain a remote access message. The remote access message is sent to the data center to initiate request for access to the postage security account by the remote user device. The remote user device is authenticated for accessing the postage security account when the data center verifies the remote access message.

Brief Summary Text - BSTX (4): Postage metering systems have been developed which employ encrypted information that is printed on a mailpiece as part of an indicium evidencing postage payment. The encrypted information includes a postage value for the mailpiece combined with other postal data that relate to the mailpiece and the postage meter printing the indicium. The encrypted information, typically referred to as

1

a digital token or a digital signature, authenticates and protects the integrity of information, including the postage value, imprinted on the mailpiece for later verification of postage payment. Since the digital token incorporates encrypted information relating to the evidencing of postage payment, altering the printed information in an indicium is detectable by standard verification procedures. Examples of systems that generate and print such indicium are described in U.S. Pat. Nos. 4,725,718, 4,757,537, 4,775,246 and 4,873,645, each assigned to the assignee of the present invention.

Brief Summary Text - BSTX (5): Presently, there are two postage metering device types: closed system and open system. In a closed system, the system functionality is solely dedicated to metering activity. Examples of closed system metering devices, also referred to as postage evidencing devices, include conventional digital and analog (mechanical and electronic) postage meters wherein a dedicated printer is securely coupled to a metering or accounting function. In a closed system, typically the printer is securely coupled and dedicated to the meter, and printing evidence of postage cannot take place without accounting for the evidence of postage. In an open system, the printer is not dedicated to the metering activity, freeing system functionality for multiple and diverse uses in addition to the metering activity. Examples of open system metering devices include personal computer (PC) based devices with single and/or multi-tasking operating systems, multi-user applications and digital printers. An open system metering device is a postage evidencing device with a non-dedicated printer that is not securely coupled to a secure accounting module. An open system indicium printed by the non-dedicated printer is made secure by including addressee information in the encrypted evidence of postage printed on the mailpiece for subsequent verification. See U.S. Pat. Nos. 4,725,718 and 4,831,555, each assigned to the assignee of the present invention.

Brief Summary Text - BSTX (7): The USPS has published draft specifications for IBIP. The INFORMATION BASED INDICIA PROGRAM (IBIP) INDICIUM SPECIFICATION, dated Jun. 13, 1996, and revised Jul. 23, 1997, ("IBIP Indicium Specification") defines the proposed requirements for a new indicium that will be applied to mail being created using IBIP. The INFORMATION BASED INDICIA PROGRAM POSTAL SECURITY DEVICE SPECIFICATION, dated Jun. 13, 1996, and revised Jul. 23, 1997, ("IBIP PSD Specification") defines the proposed requirements for a Postal Security Device ("PSD"), which is a secure processor-based accounting device that dispenses and accounts for postal value stored therein to support the creation of a new "information based" postage postmark or indicium that will be applied to mail being processed using IBIP. The INFORMATION BASED INDICIA PROGRAM HOST SYSTEM SPECIFICATION, dated Oct. 9, 1996, defines the proposed requirements for a host system element of IBIP ("IBIP Host Specification"). IBIP includes interfacing user, postal and vendor infrastructures, which are the system elements of the program. The INFORMATION BASED INDICIA PROGRAM KEY MANAGEMENT PLAN, dated Apr. 25, 1997, defines the generation, distribution, use and replacement of the cryptographic keys used by the USPS product/service provider

2

and PSDs ("IBIP KMS Specification"). The specifications are collectively referred to herein as the "IBIP Specifications".

Brief Summary Text - BSTX (13): In conventional closed system mechanical and electronic postage meters a secure link is required between printing and accounting functions. For postage meters configured with printing and accounting functions performed in a single, secure box, the integrity of the secure box is monitored by periodic inspections of the meters. More recently, digital printing postage meters typically include a digital printer coupled to a metering (accounting) device, which is referred to herein as a postal security device (PSD). Digital printing postage meters have removed the need for physical protection of the link by cryptographically securing the link between the accounting and printing mechanisms. In essence, new digital printing postage meters create a secure point to point communication link between the PSD and print head. See, for example, U.S. Pat. No. 4,802,218, issued to Christopher B. Wright et al. and now assigned to the assignee of the present invention. An example of a digital printing postage meter with secure print head communication is the Personal Post Office.TM. manufactured by Pitney Bowes Inc. of Stamford, Conn.

Brief Summary Text - BSTX (19): The present invention provides a method for securely controlling access to a mailer's account, which resides at a virtual meter data center. The present invention comprises means to authenticate a mailer, the secure distribution of mailer (user) authentication keys and the use of a secure box to execute the authentication algorithms. The database in the virtual meter data center holds the mailer authentication keys in cipher text to prevent exposure of the keys in plain text. The keys are only decrypted when used within the secure authentication box.

Brief Summary Text - BSTX (20): The present invention provides a method of remotely accessing a postage security account at a data center from a remote user device begins with a remote user assigning, or being assigned, a password to the user's postage security account at a data center. A cryptographic key corresponding to the user's postage security account is provided to the remote user device and is stored at the data center. The password and the cryptographic key are combined at the remote user device and the data center respectively to obtain a user authentication key. An authentication algorithm is performed using the user authentication key to obtain a remote access message. The remote access message is sent to the data center to initiate request for access to the postage security account by the remote user device. The remote user device is authenticated for accessing the postage security account when the data center verifies the remote access message.

Detailed Description Text - DETX (3): The accounting method for virtual postage metering system 10 may be a conventional prepayment or post-payment system. The preferred method is a prepayment method wherein each mailer is required to put a minimum amount of money into the mailer's virtual meter account. As account funds drop below a specific level a refill is charged against the mailer's account. An alternate accounting method that is suitable for a virtual postage metering system is a real-time payment method in which the amount of a transaction is charged to a mailer's credit

3

card account when the transaction occurs. This method is referred to herein as a "trickle charge" postage payment, because the mailer does not pay for postage for a mailpiece until the mailer is ready to print the mailpiece.

Detailed Description Text - DETX (5): Virtual postage metering system 10 eliminates the need to maintain and account for traditional metering devices at each mailer's site and provides flexibility for handling requests from multiple origins of deposit by each mailer. Virtual postage metering system 10 also provides value added services that are not available with conventional meter devices, such as, real-time address hygiene, direct marketing services and trickle charge postage payment. Virtual postage metering system 10 provides mailer authentication by Data Center 30 to identify mailers with valid accounts. When a mailer has been authenticated for each request, for example, by a username, password or other conventional methods, Data Center 30 services the request, and returns indicium information to the PC 20 where the indicium is created and printed on the mailpiece.

Detailed Description Text - DETX (10): In accordance with the present invention, one or more cryptographic modules, referred to herein as secure "boxes", are located within Data Center 30 and are used to perform cryptographic processes. Each secure box is a secure, tamper-evident, tamper-resistant and tamper-responding device, including a processor and memory, that stores encryption keys and performs cryptographic operations using the keys within the secure boundary of the device. Data Center 30 includes several types of secure boxes, which are described below. In the preferred embodiment, Data Center 30 includes multiple boxes of each type for redundancy and performance.

Detailed Description Text - DETX (11): Key Management System 38 includes a manufacturing box (not shown) that provides top-level keys used to generate random numbers for seeding each of the other secure boxes. By sharing cryptographic keys (secret and/or public), the secure boxes communicate securely within Data Center 30. Key Management System 38 also includes a "steel" box (not shown) that shares a common key with meter box 44 to encryptdecrypt master token keys for postage evidencing transactions for each meter account. The steel box merges a vendor key and a postal key into one record in cipher text. For each meter account, Data Center 30 creates a logical meter, i.e. a meter record, in Database Server 36 by generating a token key using the vendor and postal keys, initializing meter registers (ascending and descending), meter freshness data (described below) and other postal information as part of the meter record, and then storing the meter record in Database Server 36. Detailed Description Text - DETX (12): Data Center 30 also includes a meter box 44 that shares a secret key with the steel box for decrypting the token key encrypted in the meter record. Meter box 44 also holds the key used for digital signature of transaction records. The only other information stored in meter box 44 is freshness data for each meter record processed by meter box 44. For each postage transaction, meter box 44 generates at least one digital token or signs the postage transaction, and updates the meter record corresponding to the transaction. Each meter record in Database Server 36

4

includes postal funds as well as the token keys in cipher text. Meter box 44 uses the token keys to generate tokens, updates the postal funds in the meter record, and signs the updated meter record. In this manner, meter box 44 performs and controls the secure accounting for each transaction. Meter box 44 can also be used to verify the token or the transaction signature for verification of the postage evidencing for the transaction.

Detailed Description Text - DETX (13): Data Center 30 also includes an authentication box 40 that shares a different secret key with the steel box to decrypt a mailer authentication key stored in cipher text in Database Server 36. Authentication box 40 also executes the authentication algorithms using the decrypted authentication key to authenticate a mailer.

Detailed Description Text - DETX (17): In operation, Communication Server 32 receives a request for a meter transaction from mailer PC 20. The application software in the Function Server 34 controls the processing of the transaction request. Function Server 34 accesses mailer database 62 and meter database 60 to obtain records, including the appropriate meter record 64, corresponding to the meter account of the mailer initiating the request. Function Server 34 communicates mailer records from mailer database 62 to authentication box 40, which then authenticates the mailer requesting the transaction. Once the mailer has been authenticated, Function Server 34 communicates the appropriate meter record 64 to meter box 44, which verifies a signature and freshness data for the record. Meter box 44 decrypts the encrypted key(s) that are stored within meter record 64, performs accounting functions on the ascending and descending registers in meter record 64, and uses the key(s) to generate a token for the requested transaction. Meter box 44 then generates data for an indicium, and once again signs meter record 64. The updated and signed record is then sent back to Database Server 36 here it is stored as part of meter database 60.

Detailed Description Text - DETX (21): In accordance with the preferred embodiment of the present invention, an authentication protocol for the virtual postage metering system uses a shared secret between the Data Center 30 and a remote PC 20. To authenticate a mailer (also referred to herein as a user) to the virtual meter data center, the mailer must possess a secret key and a password. The secret key is preferably stored on removable media, such as a floppy diskette or dongle, so that only the mailer in possession of the removable media may access the account. Only the mailer knows the password. The secret key and the password are combined to form the authentication key that is used in the authentication protocol. For each mailer having a mailer account at Data Center 30, Data Center 30 stores the mailer's secret key in Database Server 36. When the mailer's account is initialized the mailers password is combined with the secret key to form the authentication key which is stored in encrypted form in mailer database 62 at Data Center 30. For subsequent communications, Data Center uses the stored authentication key, whereas PC 20 generates the authentication key using two pieces of information, i.e., the stored secret key and the user password.

Detailed Description Text - DETX (23): Referring now to FIG. 3, one embodiment of the present invention is shown wherein the password is used as a key itself for the authentication protocol. $K.sub.A$ is the secret key stored on the user's removable media and $K.sub.U$ is an authentication key derived from the user's password. $ID.sub.U$ is the user's ID, $ID.sub.DC$ is the Data Center ID, $C.sub.U$ is the user's challenge, $C.sub.DC$ is the Data Center's challenge, $[C.sub.U, C.sub.DC]K.sub.A$ denotes a digital signature of the user's challenge and the Data Center's challenge signed with the secret key, $[C.sub.DC]K.sub.A$ denotes an encryption of the Data Center's challenge using the secret key, and $[C.sub.DC]K.sub.U$ denotes an encryption of the Data Center's challenge using the authentication key. Authentication is assured by knowledge of the user's authentication key $K.sub.U$ that is established by combining $K.sub.A$ and the user's password prior to any communication.

Detailed Description Text - DETX (24): At step 100, PC 20 initiates communication with Data Center 30, sending the user's ID and the user's challenge in plain text to Data Center 30. At step 105, Data Center 30 responds with plain text of the Data Center ID, the user's ID, the user's challenge and the Data Center's challenge, and a digital signature of the user's challenge and the Data Center's challenge signed with the secret key. At step 110, PC 20 creates the user's authentication key $K.sub.U$ by combining the user's password and secret key $K.sub.A$ stored on a diskette, the distribution of which is described below. At step 115, PC 20 verifies the digital signature of the user's challenge and the Data Center's challenge using secret key $K.sub.A$. If not verified, the Data Center is alerted and the communication terminated. At step 120, PC 20 encrypts the Data Center's challenge using the user's authentication key $K.sub.U$ and encrypts it again using secret key $K.sub.A$. PC 20 then sends to Data Center 30 the user's ID, the Data Center ID, and the two encryptions of the Data Center's challenge. At step 125, Data Center 30 verifies the user's ID, the Data Center ID, and the two encryptions of the Data Center's challenge to complete authentication protocol. If not verified, PC 20 is alerted and the communication terminated. Data Center 30 creates user's authentication key $K.sub.U$ by combining secret key $K.sub.A$ and the user's password, which is stored at Data Center 30 prior to this communication, as described below in FIGS. 5 and 6.

Detailed Description Text - DETX (32): In a third method, a virtual meter public key is used to enable signup, downloads the software package. The software package includes the virtual meter public key. The mailer installs software into PC 20. The virtual postage metering system setup uses pseudorandom data (obtained from the mailer's machine or from the mailer's keystrokes) to seed a process which generates the authentication key. The mailer also chooses a password at this time. The mailer memorizes the password and the secret key is stored onto the hard drive or removable media (diskette or dongle). At signup, the mailer's sensitive data such as credit card information and the authentication key for the authentication protocol is encrypted with the virtual meter public key and uploaded to the virtual meter data center. Data Center 30 decrypts the sensitive data with the virtual meter private key and securely stores this data. A public key toolkit can provide the tools to enable this.

Detailed Description Text - DETX (33): Finally, in a fourth method for distributing keys, a client public key is used to enable signup. The mailer downloads or purchases the software package and installs the software in PC 20. Setup uses pseudorandom data (obtained from the mailer's machine or from the mailer's keystrokes) to seed a process which generates a public/private key pair. The mailer also chooses and memorizes a password at this time. At signup, the mailer uploads the client public key to the virtual meter data center. Data Center 30 generates the key for the authentication protocol, encrypts it with the client public key and returns it to the mailer. The mailer decrypts the authentication key for the authentication protocol with the client private key and splits it into the secret key and the password. The secret key is stored onto the hard drive or, preferably, onto removable media (diskette or dongle). Note that this method does not allow a natural mechanism for uploading credit card information to the virtual meter data center. A public key toolkit can provide the tools to enable this.

Claims Text - CLTX (1): 1. A method of remotely accessing a postage security account at a data center from a remote user device, the method comprising the steps of: providing a password to a user; providing to a remote user device a cryptographic key corresponding to a postage security account at a data center; combining the password and the cryptographic key to obtain a user authentication key; performing an authentication algorithm using the user authentication key to obtain a remote access message; sending the remote access message to the data center to initiate a request for access to the postage security account by the remote user device; and authenticating the remote user device requesting access to the postage security account by verifying the remote access message.

Claims Text - CLTX (8): 8. A method of remotely accessing a transaction evidencing account at a data center from a remote user device, the method comprising the steps of: providing a password to a user; providing to a remote user device a cryptographic key corresponding to the transaction evidencing account at a data center; combining the password and the cryptographic key to obtain a user authentication key; performing an authentication algorithm using the user authentication key to obtain a remote access message; sending the remote access message to the data center to initiate a request for access to the transaction evidencing account; and authenticating the remote user device requesting access to the transaction evidencing account by verifying the remote access message.